January-February 2020
ISSN: 0193-4120 Page No. 16217 - 16222

Secure File Sharing on Cloud: A Two-Factor Authentication Approach

Gaurav Verma, Department of Computer Science and Engineering, Chandigarh University, Punjab, India
Akash Singh, Department of Computer Science and Engineering, Chandigarh University, Punjab, India
Uttam Kumar, Department of Computer Science and Engineering, Chandigarh University, Punjab, India

Article Info
Volume 82
Page Number: 16217 - 16222
Publication Issue:
January-February 2020

Article History

Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 28 February 2020*

Abstract:

Cloud computing has emerged as an efficient tool for storing and sharing data among the various organizations, which provides massive storage and other benefits that make it easier to deal with real problems instead of hindered by problems of local storage and infrastructure maintenance. Although, cloud services benefit the individual and organization, it is still not considered a safe platform for sharing confidential information because the Cloud Service Provider has all the access to user's data and data is transferred using one-tier authentication. We, in this paper, propose a scheme for file transferring files on cloud FTP server using two-factor authentication along with data encryption scheme to make the process of file sharing and communication on cloud more secure

I. INTRODUCTION

Cloud computing technology is an emerging computing paradigm because of its low maintenance and effective characteristics of renting virtual storage to organizations as well as individuals. Cloud storage service gives us higher stability andefficiency in sharing data. Cloud computing has thrived because of the availability of high-capacity networks, storage devices, low cost computers, virtualization of hardware components and service-oriented architecture. With increasing demands of systems that can aid in storing and transferring confidential information fast and securely, cloud computing has emerged to be a tool of great importance because it provides important efficient services at lower cost. Clouds could be limited within an organization, that is, enterprise cloud or it may be expanded across many organizations as a public cloud. The best thing about using cloud services is that a user need not worry about direct management of the services. The prime objective of the cloud computing paradigm is to allow users to be able to take the benefits of all the technologies available as services without having deeper knowledge about each of the technology.The cloud aims to reduce the costs, and help users focus on their business instead of the being hindered by the IT barriers.

Cloud Service Providers(CSPs) like AWS, Azure etc offer many cloud services including network services and infrastructure services. These cloud services are usually hosted in data centres of the companies and can be only accessed by the company or individual by network connectivity. CSPs use different forms of services, including software which is referred to as Software as a Service (SaaS), hosting platform referred to as Platform as a Service (PaaS) and an entire networking infrastructure known as Infrastructure as a Service (Iaas).

January-February 2020
ISSN: 0193-4120 Page No. 16217 - 16222

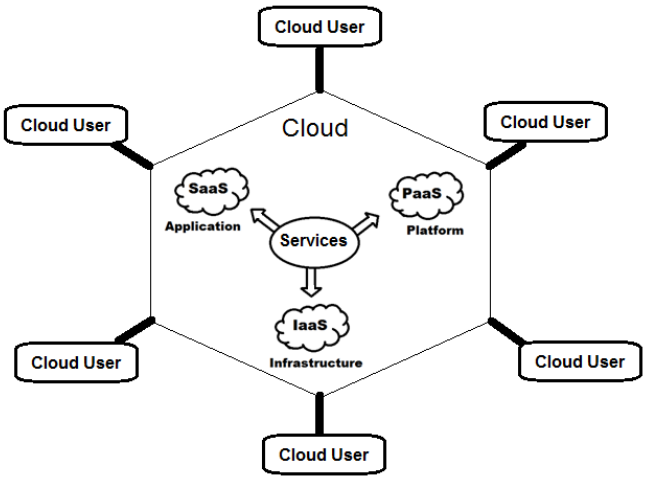

Fig.1. Cloud Computing Services

Although, CSPs provide one-tier security in file sharing process but it is not always secure enough to stop the hackers from breaching in, sometimes a more secure way is required for communication and sharing confidential data.

Nowadays, there is a demanding need of storing information in bulk and secure transferring of that confidential information all over the world. To achieve this, we use Cloud Service Provider AWS which provides a secure file sharing platform. We have our instance machine based upon a Linux backend environment.The benefit of having this file sharing directly attached with the machine is that it can be used for updating any kind of globally hosted static website or project. Moreover it's not just limited to simple sharing but along with sharing it provides a high security with good memory space. We use here the concepts of Networking, Linux environment and mainly the work is done on cloud environment. And this concept is useful in sharing & receiving files among specific users and that too involving good username and identification scenarios. We use mainly the FTP protocol and little bit of configuration task is needed to be done at sharing systems. We can also manipulate the permissions given to the different users in respect to the actions performed in context to the files. At the end security is provided by a specific random key file generated through the cloud requiring the previously mentioned username and password and the one time code shared which is only shared with the user.

II. Related Work

In the last few decades, many approaches for sharing data securely on cloud have been used and many file sharing systems and applications have beenproposed, designed and developed. Many researchers have given effective ideas and schemes for making data sharing process on cloud secure using various techniques. This section presents some works in this field that have been published by researchers.

A scheme was proposed byXuefeng Liu and YuqingZhangin, to tackle the problems like identity privacy, single-owner and static groups [2]. It was based on a model for data sharing based on multi-owner manner sharing of files where any user of the group would be able to transfer the data securely to any other user. The scheme includes data sharing with that supports dynamic groups in which users need not ask for data owners before decrypting the files. Although, their scheme covered the effective data sharing among users without much involvement of data owner to increase the identity privacy, it provides anonymity to the users to use the resources of the cloud which may lead to problems like users uploading malicious files on cloud.

People these days like to be connected 24x7 with their friends and families on social network, and in this process of socialization sharing of data takes place at great scale. There are a lot of challenges that are faced by people on the internet while using a data sharing application to either communicate or share information. Social Networking Technologies allow us to share data among our friends and family securely. Sathish Y, Balaji S and SurabhiS proposed an interactive on-demand applicationfor file sharing where users can send and receive documents and other media files by uploading them on cloud [4]. Their proposed system also included features like interacting with other people through a chat screen present in the cloud.

January-February 2020
ISSN: 0193-4120 Page No. 16217 - 16222

With increase in use of group data sharing on cloud, security and privacy have become a major concern. Cloud service providers cannot be trusted with our highly sensitive data. To overcome these challenging security concerns,KaipingXue and Peilin Hong, proposed a generalized group sharing frameworkhaving the benefits of proxy signature, enhanced TGDH (Tree-based Group Diffie-Hellman) and re-encryption proxy together [5]. Proxy signature allows group leader to grant privileges to the chosen group members, enhanced TGDH is used to update the group key pair without needing all the group members to be online at the same time, and re-encryption proxy scheme allows delegation of computational intensive operations to cloud server without revealing any confidential data.Once we upload our data on cloud, we lose the trace of the data and it is almost impossible for us to know if some unwanted personnel or a hacker gets his hands on our sensitive data, which poses a high security risk. Bharat S Rawal and S SreeVivek suggested a file sharing technique for cyber defense among different clouds without the need of sharing an encryption key [10]. Theydiscussed a mechanism for the file sharing on cloud with disintegration protocol (DIP) to transfer the files securely.Even though cloud services like massive storage management and sharing of data are enjoyed by many users, it comes at cost of sharing data with Cloud Service Providers. Unlike users, CSPs cannot be trusted to have our sensitive data. ShengminXu andGuomin Yang recommendeda scheme to protect our super-sensitive data against the unreliable Cloud Service Providers [13]. They proposed a scheme to share data at a fine-grained level among authorized users on cloud using Attribute Based Encryption (ABE) with the property of indentify based encryption.

III. Proposed work

In this work, we propose a scheme for transferring encrypted files securely using FTP server hosted over AWS platform using two-factor authentication. Most of the approaches for sharing data over cloud include the traditional authentication to verify user's identity before providing access to files, but our scheme focuses on providing more security to the user's sensitive files.Due to high efficiency and low maintenance, file sharing over cloud has become very popular in the IT world. But there is a huge risk factor in sharing important data on cloud as leak in any confidential data can lead to major issues, and that is why our approach of sharing data on cloud includes more security features to make the transfer of data safe and secure. Specifically, our data sharing model is based on combining security factors like access control, authentication and encryption together is such a way to provide security to a higher degree.

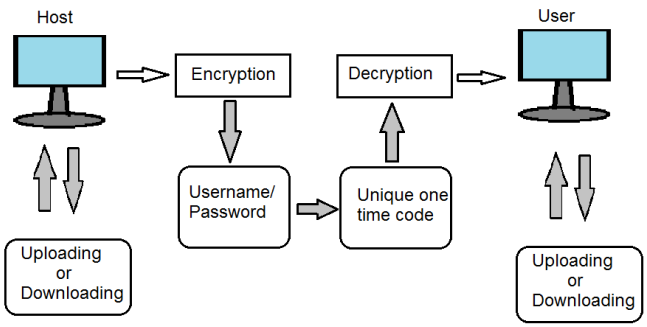

Fig.1. System model working

Amazon Web Services is a flexible platform which provides services that are easy-to-use for the users in solving cloud computing problems with minimal maintenance requirement of the resources rented by AWS. One of the most important services offered by AWS is Elastic Compute Cloud (EC2), which is a virtual machine with operating system level control. EC2 basically provides us a virtual machine OS having configuration according to our need. Creation of an instance EC2 machine over the AWS gives us our very own virtual server upon which we can run various applications in computing environment. All it needs is proper configuration of the EC2 instance according to the services we need. Once the instance is ready, we can use usual file transfer commands to share data among users group. Data to be sent is first encrypted using a simple yet powerful Advanced Encryption Standard algorithm

January-February 2020
ISSN: 0193-4120 Page No. 16217 - 16222

through OpenSSL command line on Linux OS, and then it is uploaded on cloud server. When a user needs to access the data from cloud server, he is required to verify his identity during multi-authentication processes. After the authorization is validated, user can now access the data but to read the data a decryption key is required to decipher the data from encrypted form to readable plaintext.

Authentication

Authentication is the most basic, traditional security feature available that has been used for security purpose on internet. User requires a unique username and password to be able to access to the files on cloud storage. Authentication makes sure

only the person who has the knowledge of the password assigned to the user can access the files. The apparent risk with having a single-level static authentication is if someone gets to know the password assigned to user, user's data can be compromised.

To deal with this issue, we introduce another authentication in our file sharing model. A dynamic two-factor authentication process is way better than the static one in terms of security as the pass-code or the pass-key generated every time user tries to access files is different. A randomly generated pass-key validation is required after the normal username/password authentication to get access of performing any kind of operations on cloud.

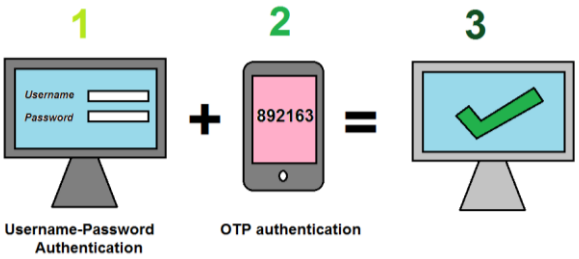

Fig.3.Two-Factor Authentication (2FA) model

Encryption

Once the identity of the user is proved, access control security comes into play to minimize the security risk. Access control technique defines whether the user has the rights or privileges to access or perform any operation on data. Access control system is responsible for authentication and authorization process by assessing the login credentials provided by user.

Authentication techniques and access control systems can secure data from unauthorized person trying to get his/her hands on confidential data but there is always a possibility that these techniques might fail to stop an intruder from breaking in and acquiring secure files. Leakage of sensitive data is a huge risk, that's why we cannot just rely on authentication and access control. Our model suggests encryption of dataAdvanced Encryption Standard (AES) algorithm before transferring which can only be decrypted using a certain decryption key which is only shared with the user. AES is a Symmetric-key algorithm which uses same cryptographic key for encrypting plaintext to cipher text and vice versa. AES cryptographic keys are normally fixed-length (128 bits or 256 bits).Encryption of data ensures that even if some intruder gets the data by invading user's privacy, he will not be able to decrypt it without the decryption key.

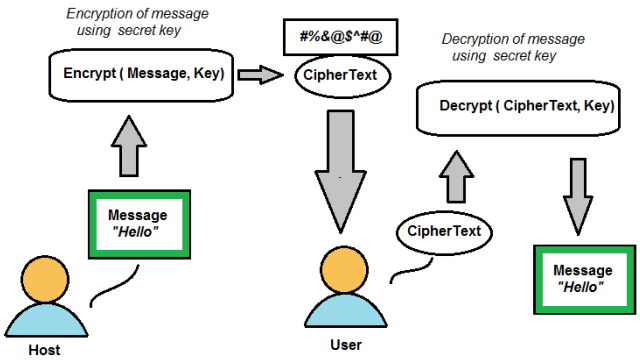

Fig.4.Symmetric-Key encryption

IV. Result and Discussion

This section of the paper shows the results of our work. We successfully implemented the encryption algorithms for symmetric-key encryption to secure

January-February 2020
ISSN: 0193-4120 Page No. 16217 - 16222

the data. The encrypted data was then transferred using a cloud file transfer protocol server.

Previous related work File Sharing on cloud

Name	File Sharing	Authentication	Encryption	OTP
Xuefeng Liu	Yes	Yes	Yes	NO
Sathish Y	Yes	Yes	NO	NO
Kaiping Xue	Yes	Yes	Yes	NO
Shengmin Xu	Yes	Yes	Yes	NO
Our work	**Yes**	**Yes**	**Yes**	**Yes**

Fig.4.Previous work comparison

As mentioned in the Fig 4. Various models and techniques related to file sharing on cloud have been proposed before our work, but what they lack is two-factor authentication. Our work includes the2FA approach to improve the security and observed its effectiveness.

VI. Conclusion and Future Work

In this paper, we propose a secure file sharing scheme using two-factor authentication and data encryption. In this model of file sharing, user can upload data on cloud server by encrypting it using a cryptographic key to prevent it from cyber-hackers. Moreover, to make the file sharing process more secure, the data downloaded from cloud needs to be decrypted using the same key in order to convert it into readable form.

Although, many attempts including the one suggested in this paper have been made to come up with strategies to make data transfer more efficient and secure on cloud, more work is still required in this field. Stronger encryption algorithms along with different security frameworks are required to be implemented to prevent our precious data from cyber attacks.

REFERENCES

[1] Lee, S., Ong, I., Lim, H., & Lee, H. (2010). Two Factor Authentication for Cloud Computing. *J. Inform. andCommun. Convergence Engineering, 8*, 427-432.

[2] X. Liu, Y. Zhang, B. Wang and J. Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 6, pp. 1182-1191, June 2013.

[3] S. Zhu, X. Yang and X. Wu, "Secure Cloud File System with Attribute Based Encryption," *2013 5th International Conference on Intelligent Networking and Collaborative Systems*, Xi'an, 2013, pp. 99-102.

[4] Y, Sathish& S, Balaji& S, Surabhi. (2014). Advanced File Sharing Using Cloud.International Journal of Engineering Trends and Technology. 15. 63-67. 10.14445/22315381/IJETT-V15P214.

[5]K. Xue and P. Hong, "A Dynamic Secure Group Sharing Framework in Public Cloud Computing," in *IEEE Transactions on Cloud Computing*, vol. 2, no. 4, pp. 459-470, 1 Oct.-Dec. 2014.

[6]Y. Zhang, F. Patwa and R. Sandhu, "Community-Based Secure Information and Resource Sharing in AWS Public Cloud," *2015 IEEE Conference on Collaboration and Internet Computing (CIC)*, Hangzhou, 2015, pp. 46-53.

[7]S. Wang, K. Liang, J. K. Liu, J. Chen, J. Yu and W. Xie, "Attribute-Based Data Sharing Scheme Revisited in Cloud Computing," in *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 8, pp. 1661-1673, Aug. 2016.

[8] N. Alhebaishi, L. Wang, S. Jajodia, and A. Singhal,"Threat modeling for cloud data center infrastructures",in*International Symposium on Foundations and Practiceof Security*, Springer, 2016, pp. 302–319.

[9] Rawal, B.S., Kalutarage, H.K., Vivek, S.S., &Pandey, K. (2016). The Disintegration Protocol: An Ultimate Technique for Cloud Data Security. *2016 IEEE International Conference on Smart Cloud (SmartCloud)*, 27-34.

January-February 2020
ISSN: 0193-4120 Page No. 16217 - 16222

[10] B. S. Rawal and S. S. Vivek, "Secure Cloud Storage and File Sharing," *2017 IEEE International Conference on Smart Cloud (SmartCloud)*, New York, NY, 2017, pp. 78-83.

[11]K. A. Torkura, M. I. H. Sukmana, M. Meinig, F. Cheng, C. Meinel and Graupner, "A threat modeling approach for cloud storage brokerage and file sharing systems," *NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium*, Taipei, 2018, pp. 1-5.

[12] S. Xu, G. Yang, Y. Mu and R. H. Deng, "Secure Fine-Grained Access Control and Data Sharing for Dynamic Groups in the Cloud," in *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 2101-2113, Aug. 2018.